AMENDMENT TO THE CLAIMS

1. (Previously Presented) A computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

pre-establishing an encryption relationship between a computing device and the biometric device, wherein the computing device and biometric device include separate but related encryption components and the biometric device encryption component is implemented as firmware and decrypts information encrypted by the computing device encryption component;

generating a session packet, wherein generating a session packet comprises generating a session number and storing it in the session packet;

maintaining a record of the session number;

encrypting the session packet utilizing the computing device encryption component and transmitting it to the biometric device;

receiving a biometric information packet from the biometric device, decrypting it, and making a determination as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet, wherein making a determination comprises comparing a session number received with or as part of the biometric information packet to the record of the session number; and

wherein pre-establishing, generating, maintaining, encrypting, and receiving enhance the security of informational interactions between the biometric device that collects the collection of biometric data and the computing device that selectively utilizes the collection of biometric data.

2. (Previously Presented) The method of claim 1, wherein the method is performed in the consecutive order of pre-establishing, generating, maintaining, encrypting, and receiving.

3. (Previously Presented) The method of claim 1, further comprising storing the session number in a database associated with the computing device.

4. (Previously Presented) The method of claim 1, wherein generating a session packet further comprises obtaining a session key and storing it in the session packet.

5. (Original) The method of claim 4, further comprising storing the session key in a database associated with the computer.

6. (Original) The method of claim 4, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption key that is complimentarily related to the session key.

7. (Original) The method of claim 4, wherein obtaining a session key comprises generating a public key portion of a PKI key pair.

8. (Original) The method of claim 7, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair.

9. (Original) The method of claim 1, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption component that is independent of the pre-established encryption relationship.

10. (Previously Presented) The method of claim 1, wherein generating a session packet further comprises generating a session time stamp and storing it in the session packet.

11. (Cancelled)

12. (Previously Presented) The method of claim 4, further comprising storing the session number, the session key and a session time stamp in a database associated with the computer.

13. (Cancelled)

14. (Previously Presented) The method of claim 1, wherein making a determination further comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

15. (Previously Presented) The method of claim 1, wherein making a determination further comprises comparing a data representation of a user's biometric information to at least one data representation of biometric information stored in a database.

16.(Previously Presented) The method of claim 1, wherein making a determination further comprises:

evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period; and

comparing a database representation of a user's biometric information to at least one data representation of biometric information stored in a database.

17. (Cancelled)

18. (Cancelled)

19.(Original) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first part of a PKI key pair with the computing device and a second part of the PKI key pair with the biometric device.

20. (Previously Presented) The method of claim 19, wherein encrypting the session packet comprises encrypting the session packet utilizing the first part of the PKI key pair.

21.(Currently Amended) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first part of a static encryption key pair with the computing device and a second part of the static encryption key pair with the biometric

device, one of the first and second parts being configured to decrypt information that has previously been encrypted utilizing the other part.

22. (Previously Presented) The method of claim 21, wherein encrypting the session packet comprises encrypting the session packet utilizing the first part of the static encryption key pair.

23-48. (Cancelled)

49. (Previously Presented) A computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

first, pre-establishing an encryption relationship between a computing device and the biometric device, wherein pre-establishing an encryption relationship comprises storing a first encryption component with the computing device and a second encryption component with the biometric device, one of the first and second encryption components being configured to decrypt information that has previously been encrypted utilizing the other of the first and second encryption components;

second, generating a session packet, wherein generating a session packet comprises generating a session encryption key and storing it in the session packet;

third, encrypting the session packet utilizing the computing device encryption component and transmitting the encrypted session packet that includes the session encryption key to the biometric device;

fourth, receiving from the biometric device a biometric information packet that is encrypted utilizing the session encryption key, decrypting the biometric information packet with an encryption key that is complimentarily related to the session encryption key, and making a determination as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet based on a content of a collection of

authentication information contained in the decrypted biometric information packet; and

wherein first, second, third, and fourth respectively correspond to the consecutive order of the computer implemented method.

50. (Previously Presented) The method of claim 49, wherein generating a session encryption key comprises generating a public key portion of a PKI key pair.

51. (Previously Presented) The method of claim 50, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair.